

**Ames Laboratory**  
**Office** Environment, Safety, Health and Assurance  
**Title** Integrated Safeguards and Security Management  
(ISSM) System Description  
**Page** 1 of 16

**Plan** 10200.029  
**Revision** 0  
**Effective Date** December 31, 2003  
**Review Date** January 1, 2006


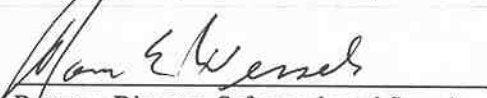

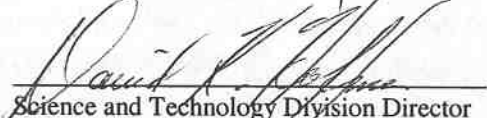

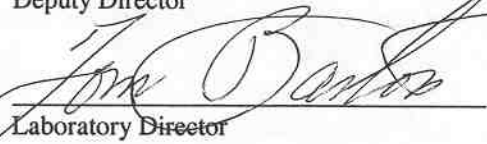
## Ames Laboratory Integrated Safeguards and Security Management System Description

The Ames Laboratory Integrated Safeguards and Security Management System Description documents the processes employed to support the principles and functions of the Department of Energy's Policy 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*.

Comments and questions regarding this plan should be directed to:

Tom E. Wessels  
Program Director, Safeguards and Security  
Manager, Environment, Safety, Health and Assurance  
G40 TASF, Ames Laboratory  
515-294-4965

### Sign-off Record:

Approved by: 	Date: <u>2/11/04</u>
Manager, Safeguards and Security	
Approved by: 	Date: <u>2/11/04</u>
Program Director, Safeguards and Security	
Approved by: 	Date: <u>2/16/04</u>
Chief Operations Officer	
Approved by: 	Date: <u>2/17/04</u>
Science and Technology Division Director	
Approved by: 	Date: <u>2/17/04</u>
Deputy Director	
Approved by: 	Date: <u>2/18/04</u>
Laboratory Director	

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 2 of 16	<b>Review Date</b>	January 1, 2006

---

## 1.0 Revision/Review Log

This document will be reviewed once every three years as a minimum.

<u>Revision Number</u>	<u>Effective Date</u>	<u>Contact Person</u>	<u>Pages Affected</u>	<u>Description of Revision</u>
0	12/31/03	T. E. Wessels	All	Original draft

## 2.0 Purpose and Scope

The purpose of the Department of Energy's Policy 470.1, *Integrated Safeguards and Security Management (ISSM) Policy* is to formalize an Integrated Safeguards and Security Management (ISSM) framework. An ISSM system framework encompasses all levels of activities and documentation related to Safeguards and Security management throughout the DOE complex and is intended to ensure the adequate protection of DOE assets (e.g., classified matter, unclassified sensitive matter, and government property).

This document describes Ames Laboratory's Safeguards and Security Management System in support of the principles and functions described in the Department of Energy's Policy 470.1. Integrated Safeguards and Security Management (ISSM) at Ames Laboratory provides a formal, organized system for planning, performing, assessing, and improving the secure conduct of work in accordance with risk-based protection strategies. It provides a road map of the Laboratory's safeguards and security related processes.

## 3.0 Background

Concerns regarding security at Department of Energy Laboratories intensified during the past few years and have been documented in several reports, including "*Science at its Best - Security at its Worst.*" In an attempt to elevate safeguards and security to the same level of concern and commitment as safety, the DOE modeled the Integrated Safeguards and Security Management (ISSM) System after the Department's Integrated Safety Management (ISM) System.

In turn, the Office of Science issued strong support for ISSM, noting there is no conflict between the goals of great science and good security and that we must do both. Specifically, Office of Science directs us to ensure that ultimately, scientists understands the security issues at stake, and incorporates these into the way they conduct their work, through the integration of science and security, in much the same way we integrate science and safety.

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 3 of 16	<b>Review Date</b>	January 1, 2006

---

## 4.0 Introduction

Ames Laboratory has a history of an organized, supportive security culture built upon sound practices and open communication of security concerns among all levels of line management. The Laboratory's Safeguards and Security Program utilizes generic security principles and graded application of DOE requirements, consistent with the inherent risks of Laboratory activities. It is designed to effectively administer processes that protect the personnel, property, facilities and information of the Laboratory. The Laboratory does not conduct classified research, does not have a classified mailing address, does not maintain security clearances for its staff members and has Category IV quantities of nuclear materials. The Laboratory's integrated organizational structure, its culture of line management responsibilities and consistent commitment create a sound foundation for Integrated Safeguards and Security Management (ISSM). Major elements of the Ames Laboratory Safeguards and Security Program are:

- **Program Management**: Program Management directs the Safeguards and Security (S&S) Program with assistance of the Ames Laboratory Safeguards and Security Oversight Committee, consisting of Subject Matter Experts who develop and implement policy and procedures, respond to requests for information, and provide personnel training.
- **Protective Forces**: Plant Protection Section, a unarmed protective force conducts facility tours, observes electronic monitoring systems, and participation in emergency responses.
- **Security Systems**: Security Systems include operating, testing and maintaining intrusion detection systems, an alarm management and processing center, protective lighting, voice communication systems, limited S&S related barrier systems such as windows, doors, closures and locks, and providing Office of Science Badges and keys.
- **Cyber Security**: The purpose of Cyber Security is to effectively detect, deter and manage undesirable and possibly malicious access to Ames Laboratory cyber information and systems. Efforts ensure protection through the development, maintenance and implementation of a Cyber Security Protection Plan (CSPP) and the training and education of personnel in network intrusion detection and prevention.
- **Personnel Security**: Personnel Security aids in protecting Laboratory employees from unnecessary risks from foreign collaborations and interfaces significantly with two programs: Foreign Travel and Foreign Visits and Assignments. The Foreign Travel program ensures that travel to and from foreign countries is reviewed and approved, information is entered into the DOE Foreign Travel Management System (FTMS), and travel alerts affecting the employee are reviewed and shared. The Foreign Visits and Assignments program includes registration of foreign visitors and assignees prior to arrival at the Laboratory and entry of vital information into the DOE Foreign Visits and Assignments Database.
- **Material Control and Accountability**: The Laboratory's Nuclear Material Control and Accountability Program is designed to control and account for nuclear materials subject to DOE Order 474.1A according to the strategic and monetary importance of nuclear materials and the consequence of their loss. It is performed to ensure nuclear materials are accounted for and unauthorized acts are detected. A complete audit trail is maintained, as required for submission to the Nuclear Material Management and Safeguards System (NMMSS).

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 4 of 16	<b>Review Date</b>	January 1, 2006

---

## 5.0 Integrated Safeguards and Security Management System Policy

The Department of Energy is committed to conducting work efficiently and securely. It is the Department's policy that the ISSM framework shall be used to systematically integrate safeguards and security into management and work practices at all levels to ensure missions are accomplished securely. Direct involvement of all personnel during the development and implementation of an ISSM framework is essential for success.

It is the policy of the Ames Laboratory to perform work securely. The Ames Laboratory ISSM system integrates safeguards and security into management and work practices at all levels so that missions are accomplished securely. This objective is fulfilled through mechanisms including policies, procedures and practices based on the following guiding principles:

- Individual Responsibility and Participation
- Line Management Responsibility for Safeguards and Security
- Clear Roles and Responsibilities
- Competence Commensurate with Responsibilities
- Balanced Priorities
- Identification of Safeguards and Security Standards and Requirements
- Tailoring of Protection Strategies to Work Being Performed

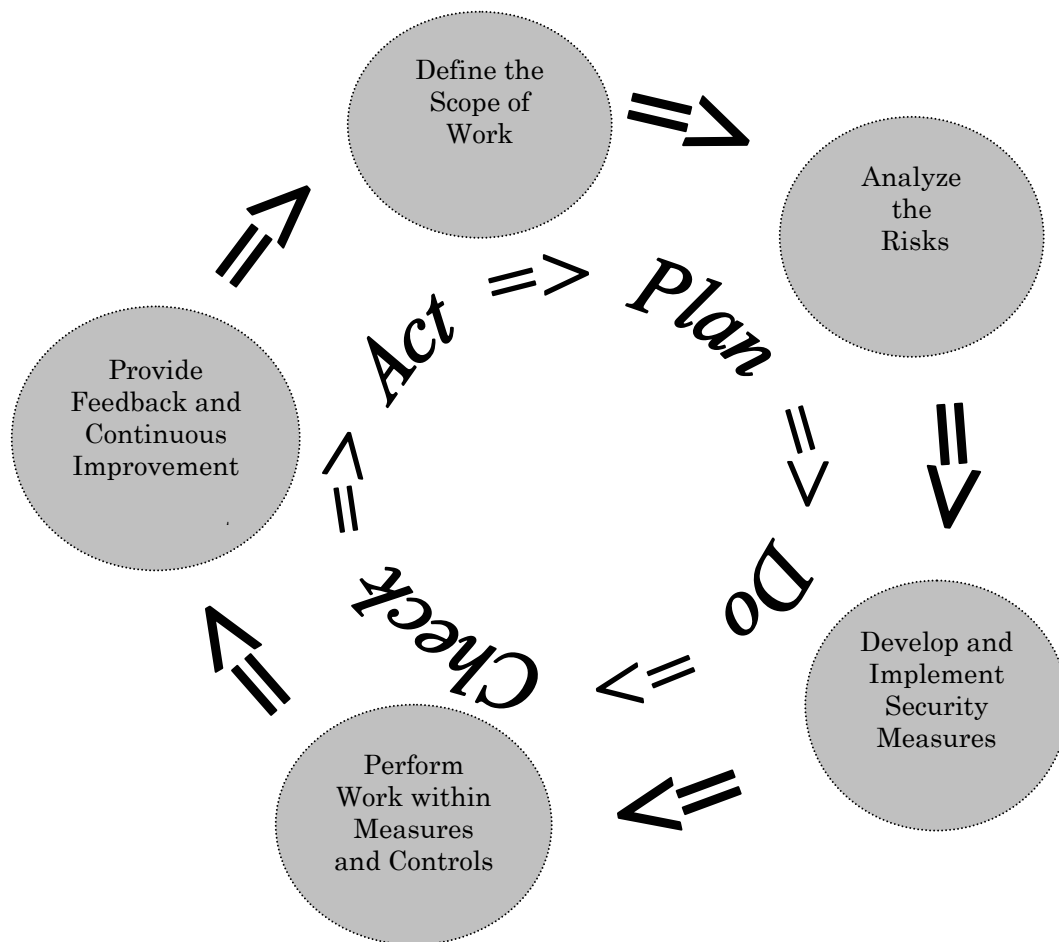
Ames Laboratory work activities that can potentially impact safeguards and security are defined, analyzed, developed, performed, and reviewed according to the Laboratory's Safeguards and Security Program. The five core ISSM functions provide the necessary structure for any work activity. The functions are applied as a continuous cycle with the degree of rigor appropriate to address the type of work activity and the risk involved. The ISSM Core Functions are:

- Define the Scope of Work
- Analyze the Risk
- Develop and Implement Security Measures
- Perform Work within Measures and Controls
- Provide Feedback and Continuous Improvement

ISSM mechanisms are the information and tools used to apply and implement the guiding principles and core functions. The Ames Laboratory's programs, policies, procedures, and practices are the mechanisms through which its ISSM system is implemented. The Laboratory's ISSM mechanisms define responsibilities and provide implementation guidance according to and sufficient for the associated risks of the work activity being performed.

## 6.0 ISSM System Performance

The Safeguards and Security practices at Ames Laboratory are based on Integrated Safeguards and Security Management principles. The Laboratory utilizes a “Plan-Do-Check-Act” approach to work activities. This “Plan-Do-Check-Act” approach is fundamental to scientific, business, safety, and security processes. The Core Functions of Integrated Safeguards and Security Management are essentially the “Plan-Do-Check-Act” cycle applied to the integration of security into planning and work performance. The Core Functions of Integrated Safeguards and Security Management are illustrated by a typical “Plan-Do-Check-Act” cycle as follows.



Key safeguards and security mechanisms (programs, policies, procedures and practices) of the Ames Laboratory Integrated Safeguards and Security Management System are described in the following sections. Often these mechanisms address several of the functions of ISSM, therefore some repetition exists within the following description.

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 6 of 16	<b>Review Date</b>	January 1, 2006

---

## 6.1 Define the Scope of Work

“Define the Scope of Work” refers to the translation of missions into work, with potential requirements identified, expectations set, tasks identified and prioritized, related security assets identified, and resources allocated.

The fundamental mechanism for definition of Ames Laboratory work at the institutional level is the GOCO contract, **Contract No. W-7405-ENG-82**. The contract provides the general guidance for operation of Ames Laboratory and includes reference to specific security obligations in **Appendix I, DOE Directives and Ames Laboratory Work Smart Standards Set**. Safeguards and Security Oversight Committee members are involved in review of contract elements and directives. In addition, the **Ames Laboratory Institutional Plan** documents the Laboratory’s mission, strategic plan, core businesses, critical success factors and resource projections. The Export Control Officer is responsible for its preparation and both the Export Control Officer and the Chief Operations Officer, who are members of the S&S Oversight Committee, review the development of the entire Institutional Plan. The S&S program director and manager are responsible for submittal to the Institutional Plan. The **Site Security Plan (Plan 10200.007)** (SSP) provides definition of the overall aspects of the Laboratory’s Safeguards and Security Program and the **Cyber Security Program Plan (Plan 50000.002)** documents the administrative, technical, and physical protection measures and procedures of unclassified cyber security controls.

The Laboratory maintains a tested and effective Emergency Preparedness Program as described in the **Ames Laboratory Emergency Plan (Plan 46300.001)** and the **Emergency Plan Implementation Procedure (Procedure 46300.010)**. The Emergency Preparedness Program is based on hazards and risks associated with Laboratory activities and non-Laboratory activities with potential to impact Laboratory facilities and personnel. **Hazard Assessments** done in 1992, 1994 and 1998 document the technical basis for the program. A **Hazard Survey Update** is conducted annually to identify any changes in the hazards at the Laboratory that would affect emergency preparedness activities. The Laboratory’s Emergency Preparedness Program is designed to address safety incidents as well as security related incidents, as defined by the Laboratory’s Safeguard and Security Program. In addition, the Laboratory’s response to **DOE N 473.6, Security Conditions, Ames Laboratory SECON Description Form (Form 10200.136)**, is coordinated with the Laboratory’s Emergency Preparedness Program.

Definition and prioritization of work, the initial scoping and the allocation of resources for research projects and support functions are achieved according to several mechanisms. These mechanisms include the **Unified Field Budget and Work Authorization Systems (WAS) Call**, the **Preliminary Proposal Form (Form 10100.001)** and the **Laboratory Directed Research and Development** process. Funded research and support function projects are reviewed according to the procedure for **Readiness Review (Procedure 10200.010)**. The Readiness Review Procedure and the ALARA committee review and approval are the primary mechanisms of planning MC&A radiological materials usage. Specific requests for service work are documented

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 7 of 16	<b>Review Date</b>	January 1, 2006

---

according to the *Service Order Requisition (Form 46200.036)*, which are reviewed by ESH&A specialists including the MC&A officer for notification of actions with potential impacts on the MC&A program. At the program level, Protective Force security issues are clarified through Readiness Reviews and situational requests from line management and resolved according to the processes described in the Plant Protection Section's *General, Post and Special Orders (Manual 10201.002)*.

The Laboratory's Export Control Officer reviews research project proposals (in-cycle and out-of-cycle) as described in the *Export Control Program Plan (Plan 10100.001)*. Notations are made on the *WAS Checklist* or the *Preliminary Proposal Form (Form 10100.001)* when Export Control requirements exist (i.e. the proposed work will not be "fundamental research"). When a project with export control requirements is funded, the principal investigator is asked to meet with the Export Control Officer, and an export control review of the proposed work is performed to determine if any part of the project would be subject to the *Export Administration Regulations (EAR)*. The review is documented using the *Export Control Review Checklist (Form 40000.001)* and is signed by both the principal investigator and the Export Control Officer. If the review determines that an Export License is required, the license application is prepared and submitted to the Department of Commerce (DOC) for approval. After the completion of the Review, the Budget Officer is notified as to any export control requirements.

Physical security systems such as intrusion detection systems, protective lighting, voice communication systems, door closures and locks are maintained through preventative maintenance tasks as initiated through the *Computer Aided Maintenance System (CAMS)* as described in the *Life Cycle Asset Management Plan (46300.002)* and the *Ames Laboratory Maintenance Manual (46300.101)*. Incidental repair issues are generally identified through *Worker Observations, Safety and Physical Security Discrepancy Reports* and *Condition Assessment Surveys*. Incidental repairs are tracked as repair tickets and funded through standing *Job Orders*. Facilities Services Group (FSG) issues keys and operates the access control system in accordance with the *FSG Office Procedures Guide* and maintains tracking and change control processes. Key and access requests generally originate from staff and are approved by Program Directors/Department Managers or authorized assistants. A lost key process is utilized to document and initiate lock replacement or acceptance of compromised security.

The *Cyber Security Program Plan (Plan 50000.002)* documents the administrative, technical, and physical protection measures and procedures of the Laboratory's unclassified cyber security controls in fulfillment of the requirements in *DOE O 205.1, Department of Energy Cyber Security Management Program; DOE N 205.2, Foreign National Access to DOE Cyber Systems; DOE N 205.3, Password Generation, Protection, and Use; and DOE N 205.4, Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*. Ames Laboratory established a Computer Protection Program Manager (CPPM) to coordinate its unclassified cyber security program. Program and Department offices appoint Assistant Computer Protection Managers (ACPMs) to assist line management fulfill cyber security responsibilities. The *Cyber Security Guide (Guide 50000.001)* documents the roles and responsibilities of laboratory personnel in fulfilling the cyber security program.

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 8 of 16	<b>Review Date</b>	January 1, 2006

---

The planning and fulfillment of human resource needs are achieved through the ***Professional and Scientific Position Information Questionnaire (PIQ)*** and the ***Position Description Questionnaire (PDQ)*** in conjunction with the ***Needs Assessment Procedure (Procedure 10200.029)***. The ***Training Needs Questionnaire (Form 10200.030)*** is utilized to document individual training needs for each employee. The ***Visitor Safety Guide (Guide 10200.001)*** provides guidance on the safety and security requirements for visitors and vendors.

The Ames Laboratory Unclassified Foreign Visits and Assignments program is structured around the requirements of ***DOE P 142.1, Unclassified Foreign Visits and Assignments***. Under this policy, the Laboratory is exempt from reporting foreign visits unless the host for the visit has access authorization (***Secretarial Memorandum dated 7/14/99***). A supplemental letter from the Ames Area Office Manager, dated 2/6/01, further amended the Laboratory's procedures by allowing foreign visitors on-site before indices checks, if required, are performed. On December 17, 2002 further guidance was issued from Kyle McSarrow that requires the Laboratory to report in FACTS certain information about our foreign national visitors and assignees that was not required under P 142.1. Essentially all foreign visitors and assignees are reported into FACTS as required by either P142.1 or the McSarrow guidance. As scientists evaluate their research plans, it is often necessary and desirable to bring foreign nationals on-site in order to improve and enhance the potential for successful outcomes. Laboratory staff collaborates with foreign nationals and find it advantageous to invite foreign scientists to come on-site to discuss projects, work on papers, give talks, and conduct other research activities. Foreign students are also important to the mission of the Laboratory by providing support to Principal Investigators and opportunities for Laboratory scientists to train the next generation of scientists. An Export Control review of the visit or assignment is initiated when the Chief Operations Officer, upon review of the ***Ames Laboratory Short Form Request for Foreign National Visit or Assignment (Form AL-473S)***, believes export control issues are involved. Generally, the requestor is notified to get clarification of the visit or assignment. If the research falls under ***Export Administration Regulations (EAR)***, a license would be requested from DOC before allowing the individual access to controlled information. If the requestor affirms that the visitor will only have access to "fundamental research", but the requestor has past or ongoing research that falls under the EAR, and the visitor is from a country for which the technology/information is subject to EAR, then a letter is sent to the requestor reminding him of his responsibilities not to share any controlled information.

The Ames Laboratory foreign travel program is structured around the requirements of ***DOE O 551.1A, Official Foreign Travel***, and ***DOE N 470.2, Reporting Unofficial Foreign Travel***. In the case of official foreign travel, the traveler must present justification that indicates the travel will support the mission of DOE and the Laboratory. Foreign travel authorization is requested on ***DOE Form 1512.1***. The completed form is routed to the Program Director for review and approval and forwarded to the Office of the Chief Operations Officer (COO). Here the form is reviewed for completeness, timeliness, and conformity with DOE guidance. If appropriate, the COO provides local approval and data from the form is input into the ***DOE Foreign Travel Management System (FTMS)*** for approval by DOE. Once the trip is approved, the traveler is



---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 9 of 16	<b>Review Date</b>	January 1, 2006

---

notified so that travel arrangements can proceed. An Export Control review of the foreign travel is initiated when the COO, upon review of the foreign travel form determines that Export Control issues may be involved. The Export Control Officer calls the travel requestor to get further clarification of what the foreign travel entails, specifically if the traveler will be presenting or discussing information or taking items that might fall under the ***Export Administration Regulations (EAR)***. If the traveler affirms that he will only be presenting or discussing “fundamental research”, but the traveler has past or ongoing research that falls under the EAR, a letter is sent to the traveler reminding him of his responsibility not to share this information with any foreign nationals from controlled countries.

## 6.2 Analyze the Hazards

“Analyze the Hazards” refers to the actions of analyzing risks associated with work to determine applicable requirements.

In 1991, the Ames Laboratory conducted a Vulnerability Assessment (VA), adopting a form and technique originally used at Fermilab. The technique used data collected from the groups and departments within Ames Laboratory to assess the value and importance of real and personal property at the site. The same concept was used to revisit the subject in 1999, although the form was altered to allow database entry and additional data regarding flammable fuel loading. Although the collected information identified spaces with high replacement cost and high programmatic impact issues, after evaluating the nature of the equipment, research, and existing protective measures, no further security controls were deemed necessary. In 2002, Ames received information from the Story County Emergency Management Agency regarding a 2001 US Department of Justice terrorism assessment of Story County. Eleven sites were ranked on the Individual Target Vulnerability Summary, with the Laboratory tying with four other sites for a fourth place ranking. One Potential Threat Element was identified in Story County, a Y2K “survivalist” group with no discernible interest in the Laboratory. Additional information has been requested from Story County. When additional information becomes available, it will be used for future updates of the Laboratory vulnerability assessment. On May 20, 2003 the Deputy Secretary issued the latest version of the Design Basis Threat (DBT). Selected members of the Laboratory’s Safeguard and Security Program reviewed the referenced DBT policy. The review was undertaken with the understanding that the DBT Policy is related to DOE assets, of which Ames does not have nuclear weapons, nuclear weapon components, chemical weapons, chemical and biological agents retained in compliance with U.S. policy and treaty regulation, nor classified matter and information. Ames does have DOE facilities, property, and limited amount of Special Nuclear Material (SNM), but, Ames Laboratory has a proven record of protection of DOE facilities, materials and property, as well as sensitive information. Based on these facts and the review discussions of the policy, it was determined that the new DBT will have no impact on the Laboratory. In 1992, 1994, and 1998 the Laboratory utilized emergency management consultants to conduct ***Hazard Assessments*** of the activities performed at Ames Laboratory, and an annual ***Hazard Survey Update*** provides additional background information. These processes and documents form the technical basis for emergency planning, safety, and

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 10 of 16	<b>Review Date</b>	January 1, 2006

---

security management activities at the institutional level as documented in the *Emergency Plan (Plan 46300.001)* and the *Site Security Plan (Plan 10200.007)*.

Institutional history, reports from the Iowa State University Department of Public Safety, data from the Local Emergency Planning Committee for Story County, and notices from DOE Security offices and the FBI are used to evaluate protective force issues associated with specific Ames Laboratory work activities. Specific issues resulting from the review of information from these sources and from Activity Readiness Reviews can result in changes to the Plant Protection Section's *General, Post and Special Orders (Manual 10201.002)*.

Research and support function projects are reviewed according to the procedure for *Readiness Review (Procedure 10200.010)*. At the program level, Protective Force security issues are clarified through Readiness Reviews and situational requests from line management and resolved according to the processes described in the Plant Protection Section's *General, Post and Special Orders (Manual 10201.002)*.

As noted in a previous section the Export Control Officer analyzes the hazards and assesses the risks associated with research projects through review of information in *WAS* and *Preliminary Proposal* requests. If necessary the principal investigator is asked to meet with the Export Control Officer for additional review.

Cyber Security system hazards are identified for each computer system at the program level and the individual level upon receipt of *CIAC (Computer Incident Advisory Capability)* notification usually based on security issues for a particular operating system. These notices are e-mailed to the CPPM and distributed to ACPMs. Network vulnerability scanning is performed with the *NESUS* application which provides information to system administrators on the corrective actions available to address detected vulnerabilities. The *Open Source Network Intrusion Detection System (SNORT)* is used to perform protocol analysis, content searching and matching. This information is indicative of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts against Ames Laboratory computer systems. The data from this system is stored for searching in a database application *Analysis Console for Intrusion Database (ACID)*. Network traffic moving into and out of the Laboratory is monitored by the network traffic application *NTOP*. The network traffic information is analyzed for potential suspicious pattern evaluation. The central e-mail system utilizes virus protection software, *Sophos*, which identifies and removes viruses from e-mail attachments prior to the delivery of the e-mail message to the client. The firewall provides initial analysis of network traffic to determine if this traffic is appropriate for passing to Ames Laboratory computer systems.

In respect to Unclassified Foreign Visits and Assignments, Principal Investigators (PI) are directed to consider the potential risks associated with interactions with foreign nationals. The impact on national security, export control issues, personal security and property concerns are considered. Foreign nationals are not allowed to perform some activities without DOE approval, while others require licenses before proceeding. Once the PI determines that a foreign national

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 11 of 16	<b>Review Date</b>	January 1, 2006

---

is the best fit for a project *Form No. AL-473S, Ames Laboratory Short Form Request For Foreign National Visit or Assignment* is filled out. This form is signed by the Program Director and sent to the COO's Office for review and approval. If necessary, the COO routes the form to the Export Control Officer to check for licensing issues. Upon approval by the COO, the *AL-473S* data is entered in *FACTS* and the host is notified. Also, Ames Laboratory works with the *Office of Counterintelligence (CI), DOE-CH* by providing lists of foreign visitors and their intended interaction and provides the opportunity to screen visitors and ask questions or provide comments concerning these foreign visitors. Such interactions help Laboratory staff evaluate potential risks involved with a specific interaction. Laboratory-wide training I provided to inform staff of the risks associated with interaction with foreign nationals.

The hazards associated with foreign travel are identified in various ways. Before approval, Program Directors examine the proposed trip for the impact on the Laboratory's mission, including the risk associated with disclosing information as a part of a collaboration or as a conference speaker. With the FTMS, the Laboratory can access US State Department notices that deal with travel issues and risks. In addition, in accordance with the agreement between DOE-CH Counterintelligence (CI) and the Laboratory the CI Office is notified of each trip. This allows DOE-CH the opportunity to brief the traveler of any risks associated with the trip.

The Readiness Review Procedure and the ALARA committee approval are the primary mechanisms of planning radiological materials usage. Specific requests for service work are documented according to the *Service Order Requisition (Form 46200.036)*, which are reviewed by ESH&A specialists including the Nuclear Materials Representative for notification of actions with potential impacts on the MC&A program.

### 6.3 Develop and Implement Security Measures

"Develop and Implement Security Measures" applies to the processes whereby measures and controls are tailored and implemented to mitigate risk, with residual risk accepted by line management.

Hazard Controls for specific activities are initially selected and developed within research groups and departments, with line management providing guidance on the implementation of tailored security measures. Security specialists, in several offices provide technical assistance and guidance. Formal reviews of activities are conducted according to the procedure for *Readiness Review (Procedure 10200.010)* for new or significantly modified activities. Formal activity reviews provide a forum for the activity supervisor, group/department personnel, safety and security specialists and engineering professionals to discuss the hazards associated with the activity, review the applicable standards, detail the required control mechanisms, and establish the related safety and security envelope.

Annually, employees of the Ames Laboratory are informed of site security practices, such as door and window security, protection of personal property, and reporting suspicious packages and people. Changes in Security Conditions (SECON) are disseminated via e-mail. Security

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 12 of 16	<b>Review Date</b>	January 1, 2006

---

concerns from the site or the surrounding University community may also be introduced at Safety Coordinator/Representative Meetings. PPS monitors the central station for door alarms in secured areas and conducts tours of the facility to assure security of doors and windows during off-hours. Tours allow the officers to assess the facility for suspicious packages and people.

The Safeguards and Security Committee, Facilities Services Group, and Environment, Safety, Health and Assurance develop physical security measures and requirements. Emergency plans and procedures are developed with the guidance of the Emergency Coordinator and with input from Emergency Team members and the Emergency Planning Committee.

Cyber security is based on a managed process of network services and access controls implemented on the firewall and routers. Cyber security staff monitors network activity through the NTOP traffic analyzer and performs quarterly scans which provide timely information on computer security vulnerabilities, potential vulnerability impact, and the actions required to mitigate threats. Cyber security staff monitors network activity and information from incident advisory centers that identify and define network vulnerability threats and suspicious activity.

Principal Investigators work with various offices within the Laboratory to develop and implement hazard controls. These controls include limiting access to space, equipment and resources on an as-needed basis through key access controls. Cyber system administrative processes are utilized to control access to computers and data. Perceived risks associated with a foreign trip help to determine the controls that are implemented. Some considerations may be where to travel or when. Others may include screening the files on a notebook computer to make sure that no sensitive data is taken on trip. The traveler is responsible to travel in a manner that is as safe as possible and only share information intended to be shared.

The Laboratory counterintelligence plan includes annual counterintelligence training. This training presents the employee's responsibility to report any unsolicited contacts by anyone, including foreign nationals. The counterintelligence training also discusses close relationships with foreign nationals and associated risks. The training helps the traveler stay out of compromising situations.

Radiological materials are controlled primarily as documented in the *Ames Laboratory Radiation Safety Manual (Manual 10202.001)*, which is compliant with 10 CFR 835. Also, MC&A materials are controlled as documented in the *Materials Control and Accountability Program Plan (Plan 10202.002)*, which is compliant with DOE Order 474.1A.

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 13 of 16	<b>Review Date</b>	January 1, 2006

---

## 6.4 Perform Work within Measures and Controls

“Perform Work within Measures and Controls” relates to the performance of work according to agreed upon and authorized security measures.

The PPS supervisor evaluates the printout from the central station for security, fire and safety issues. Also, the Post 1 Log is read routinely, and interviews are conducted with all three shifts to provide oversight and assurance of compliance. This confirms the PPS officers are performing to expectations, and assesses the condition of physical security devices as well as the level of security practice of Ames Laboratory staff.

Facilities Services Group issues keys and operates the access control system in accordance with the FSG Office Procedures Guide. It documents procedures for issuance of keys with Program Director authorization, tracking, and change control. The components of infrastructure that contribute to physical security are maintained by the FSG and through maintenance contracts. These components include doors and locks, the access control system, and the central monitoring and alarm system. The *Life Cycle Asset Management Plan (46300.002)* and the *Ames Laboratory Maintenance Manual (46300.101)* describe these activities including responsibilities, methods, and feedback mechanisms.

Authorization to open a computer system to Internet access is granted once the requester completes the *Ames Laboratory Internet Accessible System Authorization form (Form 48400.003)* and the *Generic Risk Assessment/Threat and safeguard Analysis form (Form 48400.0013)*. Signature authorization denotes that each system is appropriately patched with the latest security modules for that operating system. General network services access is obtained after the completion of the *Request for New Account form (FORM 48400.0016)* and the *Request for IP address form (Form 48400.017)*.

The host obtains authorization for a foreign national visit to commence upon issuance of an approved copy of the *Short Form Request For Foreign National Visit or Assignment (Form AL-473S)*. The visitor is allowed on site after approval is issued. Controls are developed typically with input from the a variety of sources, including Program Director, Principal Investigator, Export Control Officer and Cyber Security personnel.

Once final DOE approval is received for foreign travel, the traveler completes the *Travel Worksheet, Planned Itinerary, Form 58700.001*. This worksheet is used to prepare the *Out-Of-State Travel Authorization* form, which documents Laboratory approval. This final authorization serves as the travel “orders” which the traveler needs to start the trip. It is the responsibility of the traveler to conduct their trip in accordance with the controls placed on the activity.

Radioactive materials accountable under the Materials Control and Accountability Program are kept within a secured storage area. In addition to security controls, appropriate exposure

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 14 of 16	<b>Review Date</b>	January 1, 2006

---

controls are implemented. Annual physical inventories are performed and quarterly reports are issued to DOE.

## 6.5 Provide Feedback and Continuous Improvement

“Provide Feedback and Continuous Improvement” relates to the gathering of feedback information on the adequacy of measures and controls, the identification and implementation of opportunities for improving the definition and planning of work and the sharing of best practices and lessons learned.

Ames Laboratory utilizes several mechanisms to ensure appropriate feedback and continuous improvement efforts are carried-out. The most important and effective process for identification and correction of deficiencies is observation by individual employees. Employees are charged with the responsibility of continuously assessing their individual performances and their workspaces in order to prevent problems and to identify nonconforming conditions and opportunities for improvement. A *Worker Observation Guide (Guide 10200.003)* is available to assist workers in the observation of activities within office spaces and laboratory/shop spaces. Resolution of concerns should occur at the level of line management most directly responsible for the activity. If the issue cannot be resolved at this level, the employee is directed to proceed within his line management structure or to report the concern as part of the *Employee Safety and Security Concerns Program (Plan 10200.008)*. During *General Employee Training (GET)* all employees are apprised of these rights and responsibilities and the right to contact DOE directly.

In addition, Safeguards and Security specialists review numerous transactions and activities for noncompliances and opportunities for improvement. For example, the Export Control Officer reviews all research project proposals (in-cycle and out-of-cycle). An Export Control review of a visit or assignment is initiated when the COO, upon review of the FVA form, determines that export control issues may be involved. Also, an Export Control review of foreign travel is initiated when the COO, upon review of Foreign Travel request, determines that export control issues may be involved. Additional FVA program feedback includes debriefings conducted by the DOE-Counterintelligence Officer and communications with other research staff.

Foreign Travel feedback information is used to help support current and future travelers. At the conclusion of a foreign trip the traveler prepares and submits a Foreign Travel Trip Report. This report includes information such as: dates and location of travel, contacts, topics of discussion, mission alignment, opportunities for future research, safety concerns, and other information that the traveler feels is appropriate. Foreign Travel Trip Reports are reviewed to the COO and submitted by DOE for review. An additional feedback mechanism exists through the DOE-Counterintelligence Officer’s debriefing with the traveler. This is less formal than the trip report process but covers a few different topics than covered in the trip report.

Feedback and improvement mechanisms for PPS related activities are addressed as soon as detected by the PPS supervisor. Issues of interpretation are documented and posted with sign-off by all officers. Significant issues are incorporated into the Post Orders at the next document

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 15 of 16	<b>Review Date</b>	January 1, 2006

---

review. Security issues related to the practices of other Ames Laboratory staff are documented by the PPS officer making the discovery, and mailed to the appropriate line manager the next workday, then tracked on a database. Security devices needing repair are documented and forwarded to FSG by phone, e-mail or printed report the next workday. Biennially, the Property Management group conducts inventories of Sensitive and Capital property, to evaluate loss. Information on loss from the inventories is used to determine the effectiveness of property security practices.

The Emergency Plan and Emergency Plan Implementation Procedure are reviewed annually. Emergency Readiness Assurance Plans are submitted to DOE annually. An annual assessment of the emergency preparedness program is conducted and reviewed by the Emergency Planning Committee. Annual drills and exercises are evaluated and improvements are made as needed. Evaluation, comment, and improvement is built into maintenance activities as described in the *Ames Laboratory Maintenance Manual (46300.101)*. These feedback mechanisms are built into both preventative and corrective maintenance activities.

Vulnerability notices from the authorized incident advisory center, CIAC, and results from scheduled network vulnerability scans are sent to system administrators and ACPMs. Vulnerability information with corrective action is available for review on the Cyber Security web pages located on the Laboratory's internal web server. System administrators are required to respond in a timely manner with a corrective action plan as defined by the *Ames Laboratory Systems Assessment Measures: Cyber Security* in the contract. The system administrator for individual or multi-user computer systems installs virus protection software that will catch and remove viruses. In addition, the system administrators regularly audit and update their system with necessary patches to address vulnerabilities.

Cyber Security incidents are reported internally to the Program Director and the Manager of the Safeguards and Security Program, the Laboratory Deputy Director, the DOE-CH Cyber Security contact and the Computer Incident Advisory Capability (CIAC) following DOE N 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*.

The usage of radiological materials and particularly MC&A materials is reviewed internally in fulfillment of requirements of 10 CFR 835 and DOE Order 474.1A. In addition, numerous feedback and improvement methods utilized at the Laboratory include components with overlap with radiological and materials control concerns. The Laboratory's Radiation Safety Officer also functions as the Nuclear Materials Representative, and therefore has direct involvement with all radioactive materials activities. Annual physical inventories are performed and quarterly reports are issued to DOE. DOE conducts a biennial Safeguards and Security Inspection of the Laboratory's MC&A program.

The ESH&A office administers additional safety reviews. *Independent Walk-Throughs (Procedure 10200.021)* are performed for each Program and Department on an annual basis. The Independent Walk-Through team includes a member of the Executive Council. Ames Area

---

<b>Ames Laboratory</b>	<b>Plan</b>	10200.029
<b>Office</b> Environment, Safety, Health and Assurance	<b>Revision</b>	0
<b>Title</b> Integrated Safeguards and Security Management (ISSM) System Description	<b>Effective Date</b>	December 31, 2003
<b>Page</b> 16 of 16	<b>Review Date</b>	January 1, 2006

---

Office and DOE-CH generally participate in these walk-throughs. A corrective action database is utilized to track and document close out of concerns.

Incident and accident information is developed according to the requirements of the procedure, *Accidents, Incidents & Employee Safety Concerns: Classification & Investigation (Procedure 10200.038)*. Occurrence reporting is achieved according to the *Event Reporting Program (Plan 40000.001)*. Corrective Action Plans are developed according to the requirements of *Corrective Action Development (Procedure 10200.039)*. Lessons learned from internal and external events are distributed according to the elements of the *Lessons Learned Program Implementation Plan (Plan 10200.020)*.

Information from the various feedback mechanisms described above is reviewed according to the procedure for *Trend Analysis of ES&H Concerns (Procedure 10200.041)*. This review is included as part of an annual self-assessment process as detailed in *Appendix B, Performance Objectives and Measures (Contract No. W-7405-ENG-82)*.

## 7.0 Post Performance Activity

On-going surveillance activities of the Ames Area Office, DOE-CH, and Ames Laboratory provide measurement of the effectiveness of the Ames Laboratory ISMS. Specific aspects of the Ames Laboratory ISMS are documented in the annual Laboratory ES&H Self-Assessment Report.

## 8.0 Additional Information

Additional program information that supports the Ames Laboratory Integrated Safeguards and Security Management System is documented in the Laboratory's *Site Security Plan (Plan 10200.007)*.

## 9.0 References

- DOE Policy 470.1 *Integrated Safeguards and Security Management (ISSM)*